icomera

moovbox™

MoovAdmin
Reference Guide

©2010 Icomera AB. All rights reserved.

Under the copyright laws, this manual may not be copied, in whole or in part, without the written consent of Icomera. Your rights to the software are governed by the accompanying software licence agreement. Every effort has been made to ensure that the information in this manual is accurate. Icomera is not responsible for printing or clerical errors.

Icomera AB
Vikingsgatan 3
SE 411 04 Göteborg
Sweden
Telephone +46 31 799 21 00
Email support@icomera.com

The Icomera and Moovbox logos are a trademarks of Icomera AB. Moovbox, MoovCare, MoovAdmin, and MoovManage are trademarks of Icomera AB. Other company and product names mentioned herein are trademarks of their respective companies. Mention of third-party products is for informational purposes only and constitutes neither an endorsement nor a recommendation. Icomera assumes no responsibility with regard to the performance or use of these products.

August 2010 Concurrent Firmware – 1.9.0

Contents

Contents 3

1 Device Settings 5
- 1.1 WAN Modem . . . 5
- 1.2 General . . . 7
- 1.3 Dual WAN (M200/M220 only) . . . 9
- 1.4 MoovManage . . . 10
- 1.5 DMZ . . . 10
- 1.6 SNMP . . . 11
- 1.7 Connectivity Test . . . 12
- 1.8 GPS Coordinate Transmission . . . 12
- 1.9 GPS Over IP Server . . . 14

2 Bridge Groups 16
- 2.1 Add/Edit Bridge Group . . . 17
- 2.2 Captive Portal . . . 19

3 Interfaces 22
- 3.1 State . . . 23
- 3.2 Bridge Group . . . 23
- 3.3 Wireless . . . 23
- 3.4 WAN . . . 25
- 3.5 Isolating Third Party Devices for Security Purposes . . . 27

4 VLANs 28

5 Virtual APs 29

6 Routing Table 30

7 Wireless Clients 31

8 Tunneling 32

9 Port Forwards 33
- 9.1 Port Forwards . . . 34
- 9.2 Add Port Forward . . . 34

9.3 Source 34
9.4 Original 35
9.5 New 36

10 Static Routes **38**
10.1 Static Routes 38
10.2 Add Static Route 38

11 Status **40**

12 Restore **42**

13 Reset **43**

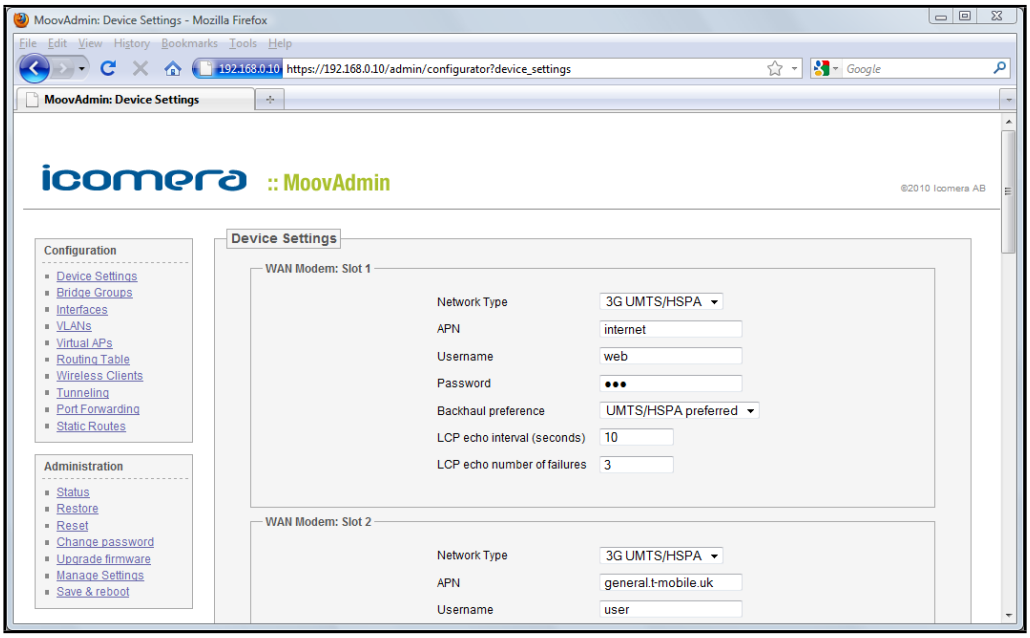
14 Change Password **44**

15 Upgrade Firmware **45**

16 Manage Settings **46**

17 Save & Reboot **47**

1 Device Settings



1.1 WAN Modem

The WAN (Wide Area Network) modem is a user-supplied device that is installed in the Moovbox and provides a data connection from your chosen carrier. The Moovbox supports a wide range of WAN modems from different vendors, as well as different technologies such as 3G UMTS and HSPA, Flash OFDM, TD-CDMA, and WiMAX. Support for new modems is being added on a regular basis, so check with your Icomera Channel Partner for more information. The Moovbox supports PC Cardbus modems natively, and ExpressCard modems with the use of a Cardbus > ExpressCard adapter.

Note: If you have an M200 there will be 2 WAN Modem sections, Slot 1 and Slot 2. These are used to configure the settings for each WAN modem separately.

Network Type

Select the type of network used by your modem.

APN, Username and Password

The APN (Access Point Name) is the name of your carrier's network. Ensure that you enter the APN, Username and Password correctly otherwise the Moovbox will not be able to establish a connection. Hint If you are not sure what APN to use, an extensive list of international carrier APNs can be found at http://www.taniwha.org.uk/gprs.html

Backhaul Preference

If you are using a 3G UMTS or HSPA modem that also supports GPRS you can use Backhaul Preference to set whether the Moovbox automatically switches to the best available network. Before you set this option, check with your carrier on the availability of 3G/HSPA coverage in the area in which you plan to operate the Moovbox. If there is complete 3G coverage, select '3G Only'. Alternatively, choosing '3G Preferred' would prioritise 3G/HSPA but allow the connection to fall back to GPRS when 3G/HSPA coverage is not available.

Note: If you select '3G Only' and the Moovbox travels out of range of the 3G network, it will not fall back to GPRS and the data connection will be lost.

Note: If you are using an alternative WAN technology such as TD-CDMA or WiMAX, the Backhaul Preference setting has no effect.

LCP

The Moovbox LCP (Link Control Protocol) feature sends an LCP echo to your mobile carrier's PPP server; if it does not receive a reply to a user-defined number of requests within a user-defined period, the Moovbox will terminate the link and initiate a new connection to the carrier network.

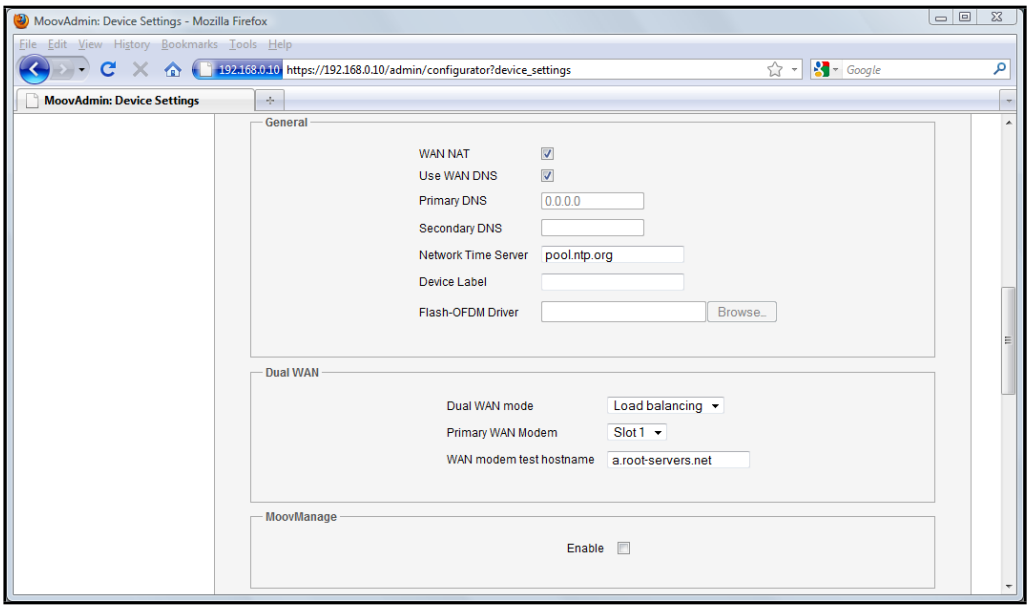
LCP Echo Interval

The Moovbox will send an LCP echo request to the carrier at the defined frequency in seconds. Normally the carrier's PPP server should respond to the echo request by sending an echo reply.

LCP Number of Failures

The Moovbox will presume the WAN connection to be dead if the defined number of LCP echo requests that are sent without receiving a valid LCP echo reply. If this happens, the Moovbox will terminate the connection and reinitiate. Use of this option requires a non-zero value for the LCP Echo Interval parameter.

1.2 General



WAN NAT

By default this option is turned on and enables Network Address Translation on the IP address issued to the Moovbox data card by your carrier. Unless you have a specific reason for turning NAT off (for example, when using a custom APN assigned to your organization by your carrier), this option should be turned on. Disabling NAT may result in you being unable to connect to the internet.

Use WAN DNS

The Moovbox will acquire its DNS settings from the carrier, removing the need to enter DNS information manually.

Primary and Secondary DNS

If you wish to override your carrier's DNS manually, uncheck Use WAN DNS and enter the primary and secondary DNS server addresses here.

Tip: Make sure you enter the DNS addresses correctly otherwise while your Moovbox will be able to connect, you will not be able to browse the Internet.

Network Time Server (NTP server)

The Moovbox is configured by default with the NTP server pool.ntp.org. This time server will be sufficient in most circumstances. If you wish to use your own NTP server enter it here.

Note: MoovManage and the VPN Tunneling feature will not function correctly if a valid NTP server is not used.

Device Label

The name you enter here will be shown at the top of the left-hand menu bar and helps you differentiate between multiple devices.

Flash-OFDM Driver

If you intend to use a Flash OFDM data card and carrier with your Moovbox you must upload the Flash OFDM driver provided by your Flash OFDM carrier. To configure the Moovbox for Flash OFDM select Flash-OFDM from the Network Type and upload the driver.

1.3 Dual WAN (M200/M220 only)

Dual WAN Mode

The Moovbox supports 3 different modes when using multiple modems. You can select between these with the Dual WAN mode option.

- *Load balancing* (M220 only) shares the traffic over both modems. For each IP accessed it randomly assigns the connection to one modem. This will spread the traffic over both modems.
- *Failover mode* uses one modem at a time. It will always use the Primary modem unless it detects that it is disconnected where it will switch over to the second modem.
- *Bridge mode* uses both modems. You can then select which bridge groups page will use which modem. Failover mode will use one modem at a time. It will always use the Primary modem unless it detects that it is disconnected where it will switch over to the second modem. Bridge mode uses both modems. You can then select which bridge groups page will use which modem.

Primary WAN Modem

When in failover mode, this enables you to select which modem is the primary WAN modem.

WAN modem test hostname

Failover mode probes the DNS servers to detect if the Primary WAN modem is active. This field enables you to change the hostname which is looked up. The default is a.root-servers.net and should not normally be changed as all DNS should resolve this address correctly.

1.4 MoovManage

MoovManage is an optional subscription-based managed service that enables you to remotely manage multiple Moovbox devices via a secure web interface. The service gives you an at-a-glance operational overview of your Moovbox devices showing availability, uptime and network (Wi-Fi and WAN) usage. MoovManage also offers a captive portal for service branding, obligatory terms of use acceptance, and Wi-Fi user authentication. The optional moovTrac module utilizes the Moovbox built-in GPS to add real-time tracking, showing group or individual Moovbox locations on a moving map. In addition, the Route Survey feature allows you to perform a WAN signal analysis of a journey and visualize the results in Google Earth.

If you have subscribed to MoovManage, you should enable MoovManage by ticking the checkbox. Apply the settings and save and reboot the device.

To monitor your Moovbox remotely, use the URL and login credentials provided to you in your MoovManage Welcome email.

If you are interested in subscribing to MoovManage or the moovTrac option, please contact your supplier or for more technical information visit the Icomera web site.

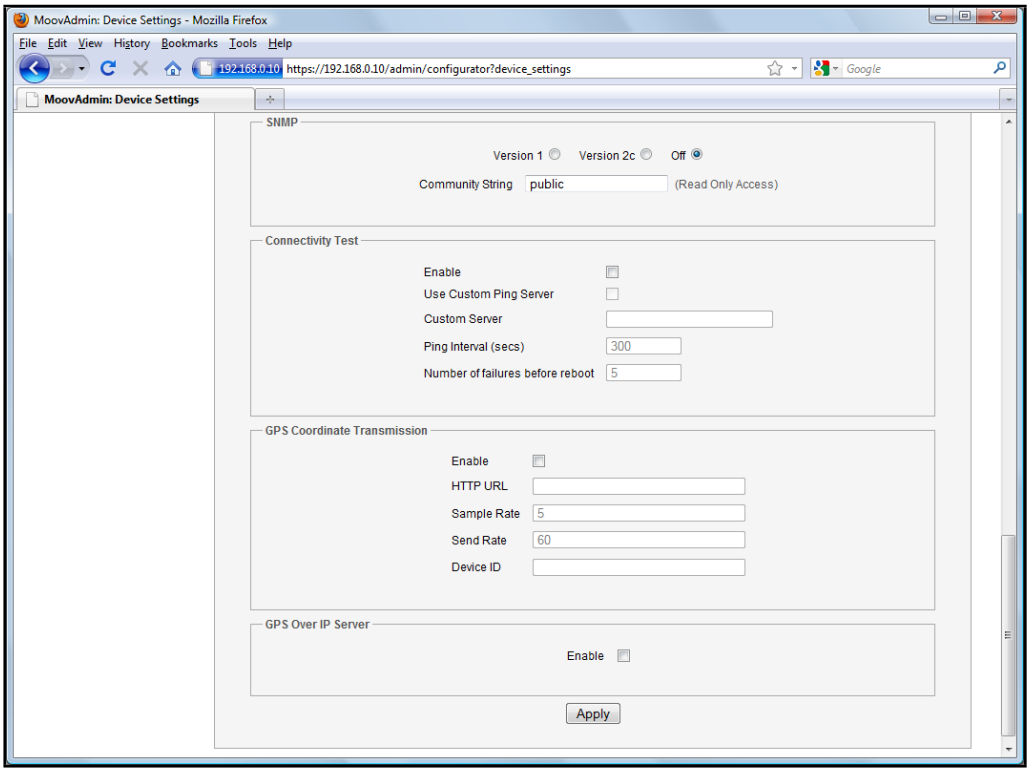
1.5 DMZ

By default this option is off. In the context of the Moovbox, when this option is enabled, all inbound traffic is diverted to the host address specified in this field. This could be a third party device such as a router, telematic or security equipment.

Note: The DMZ option only works if you have a static IP address assigned to your WAN modem. Check with your mobile carrier whether static IPs are available with your data subscription.

Tip: If you cannot obtain a WAN static IP but want to remotely access and control the Moovbox or equipment connected to it, you can use the inbound VPN function to do this. Contact your supplier or visit Icomera's support site to acquire the Moovbox VPN Tunneling Reference Guide.

1.6 SNMP



SNMP is used by network management systems to monitor network-attached devices for conditions that warrant administrative attention. It consists of a set of standards for network management, including an Application Layer protocol, a database schema, and a set of data objects. Enable SNMP either version 1 or version 2 depending on your network setup. The default read community string is set to 'public', Icomera advises this string is changed for security purposes.

1.7 Connectivity Test

This feature enables the Moovbox to ping a remote server at a user-defined interval. After a user-defined number of ping failures, the Moovbox will automatically reboot. By default this option is on, and pings a server located within Icomera's UK data center. However the test can be configured to work with a custom server by checking the Use Custom Server option and entering the network address of the target server in the Custom Server field.

Note: If you use the Custom Server option you should ensure that the target server is reliably operational and online to the public Internet, otherwise your Moovbox may reboot unexpectedly and frequently.

1.8 GPS Coordinate Transmission

The Moovbox M Series has a built-in GPS receiver for real-time positioning. If you subscribe to MoovManage with the moovTrac option, the Moovbox coordinates will be automatically sent to your MoovManage account without needing to configure anything in this pane.

If you wish to integrate your Moovbox with a third party tracking solution, enabling GPS Coordinate Transmission will send information to a remote server as an HTTP POST in XML format. This information includes time stamp, latitude, longitude, altitude and speed. The third party application will need to be able to parse the data and interpret it as a supported device type.

HTTP URL

Enter the URL of the target server location to where you want the HTTP POST request to be sent. This can be either HTTP or HTTPS; FTP URLs are not supported. The HTTP POST is in the following format:

```
<gps id="...">
  <coordinates>
    <coordinate>
      <fix>...</fix>
      <time>...</time>
```

```
      <latitude>...</latitude>
      <longitude>...</longitude>
      <altitude>...</altitude>
      <climb>...</climb>
      <speed>...</speed>
      <separation>...</separation>
      <track>...</track>
    </coordinate>
  </coordinates>
</gps>
```

The ellipses represent values that will be filled with data once the HTTP POST is made. Most are standard decimal values with the exception of:

Fix - either 0 for no GPS signal, 2 for 2D fix, or 3 for 3D fix (depending on the number and strength of satellite signals)

Time - UNIX time (i.e. number of seconds since midnight UTC of Jan 1st 1970)

Sample Rate

This setting determines how often GPS coordinates are sampled, defined in seconds. The default is every five seconds.

Send Rate

This setting determines how often the Moovbox sends the HTTP POST to the remote server, defined in seconds. GPS data is collected with the regularity defined by Sample Rate, and cached until sent to the server with the regularity defined by the Send Rate. The default is every sixty seconds.

Device ID

This setting enables the HTTP POST to be tagged with a unique alphanumeric identifier. This will identify which Moovbox the post has come from.

The Device ID is separate from the Device Name specified in the General Settings.

1.9 GPS Over IP Server

We have a TCP based GPS server running on the Moovbox on port 5050.

The server does not constantly output data; it only returns data when you send it a command. Commands are individual ASCII characters.

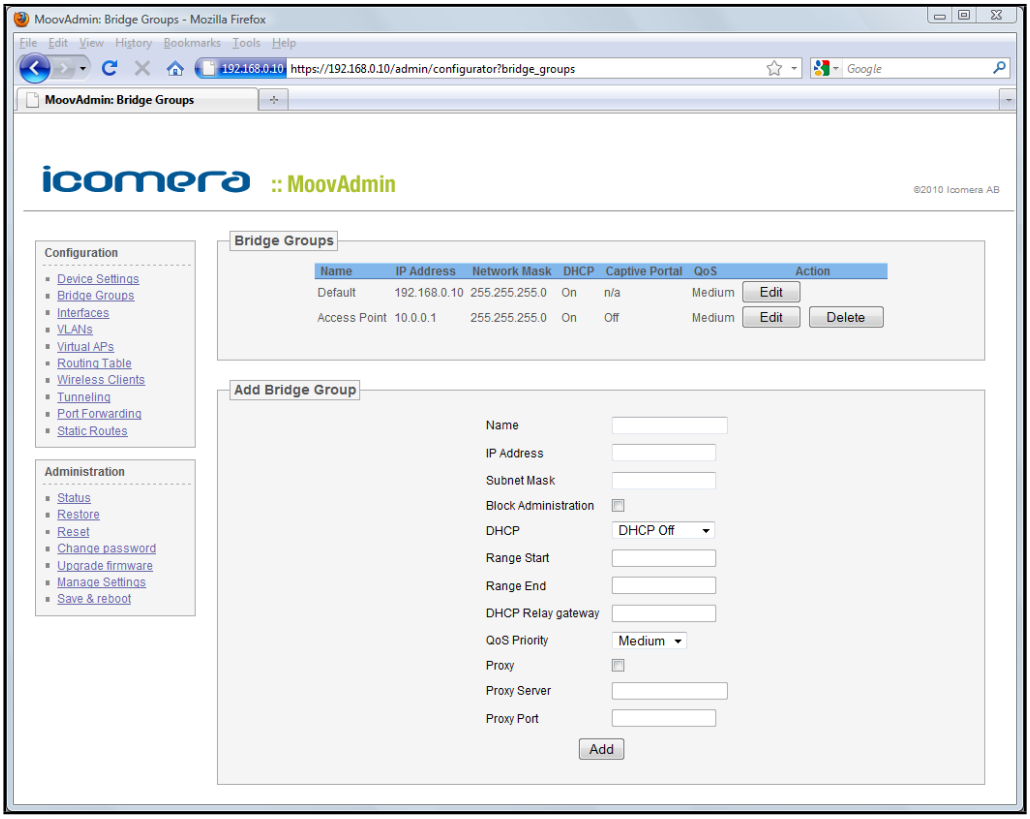
The GPS server supports two commands, 'S' returns status information and 'L' returns the location.

```
'S' returns status information

Return String:
S:init_ok,satellites_in_view,antenna_status,gps_status_code

init_ok: 0 = GPS not initialised, 1 = GPS initialised
satellites_in_view: The number of satellites in view
antenna_ status: 0 = Antenna OK, 1 = Antenna open fault, 2 = Antenna
short fault
gps_status_code:
0 = Doing position fixes
1 = Don't have GPS time yet
2 = Need initialization
3 = PDOP is too high
8 = No usable satellites
9 = Only 1 usable satellite
10 = Only 2 usable satellites
11 = Only 3 usable satellites
12 = The chosen satellite is unusable

'L' returns the location

Return String:

L:fix_type,time,latitude,longitude,altitude,climb,speed,separation,track
fix_type: 0 = No Fix, 2 = 2D Fix, 3 = 3D Fix
```

```
time: The time as a unix timestamp (seconds)
latitude: Latitude in decimal degrees
longitude: Longitude in decimal degrees
altitude: Altitude in meters
climb: Up velocity in meters per second
speed: Speed in knots
separation: The difference between the WGS-84 earth ellipsoid and mean
sea level (meters)
track: The direction in degrees
```

The internal update rate is every second, but theoretically you can request data as often as required as there is no response rate limit.

2 Bridge Groups



On the Moovbox each interface is connected to a bridge group. A bridge group bridges the interfaces together so that multiple interfaces appear as one logical interface. By default the Moovbox ships with one bridge group 'Default' that routes the both the Ethernet and Wi-Fi interfaces to the WAN modem, and enables DHCP (in the same range) for any devices connected to either interface. There may be scenarios where you want to create separate bridge groups for the Ethernet and Wi-Fi interfaces. You create a new bridge group first, and then assign it to a specific interface via the Interfaces section (see page 14).

2.1 Add/Edit Bridge Group

Name

Set the name as something meaningful as it will appear in the group setup of the network interfaces.

Tip: At support.icomera.com you can download sample configuration files that will set up your Moovbox for the most common applications.

IP Address & Subnet Mask

Each bridge group requires an IP address. The Moovbox will handle all the routing between the bridge groups.

Tip: Set each bridge group with its own IP subnet. The Moovbox will not function properly if multiple bridge groups use the same IP range.

Block Administration

This option blocks access to the MoovAdmin from the interface within the bridge group. For example, as a security measure you can block administration over the wireless interface when deploying the Moovbox for public Wi-Fi applications.

Note: It is not possible to block administration on the Default bridge group as this could potentially result in the Moovbox becoming inaccessible.

DHCP

DHCP is a protocol used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server.

Select Use DHCP for standard DHCP, or DHCP Relay if you are using a DHCP relay server.

Tip: Make sure the DHCP range is within the subnet mask specified above. You must tick the DHCP check box before you can specify a DHCP range.

Range Start

DHCP start range is the first address given out by the Moovbox, for example 10.0.0.100.

Range End

DHCP end range is the last address given out by the Moovbox, for example 10.0.0.250.

DHCP Relay gateway

Enter the IP address of a DHCP relay. The Moovbox must be addressable from the DHCP relay server and cannot be behind NAT.

QoS Priority

Quality of service or QOS gives you the ability to provide different priority to traffic travelling over the specified bridge group. Setting a bridge group with High priority will take preference over medium priority and medium over low.

Tip: If you are using your Moovbox with a single data card and have devices connected locally via Ethernet, Icomera recommends setting the Ethernet group (default group by default) to high priority to guarantee a better level of service.

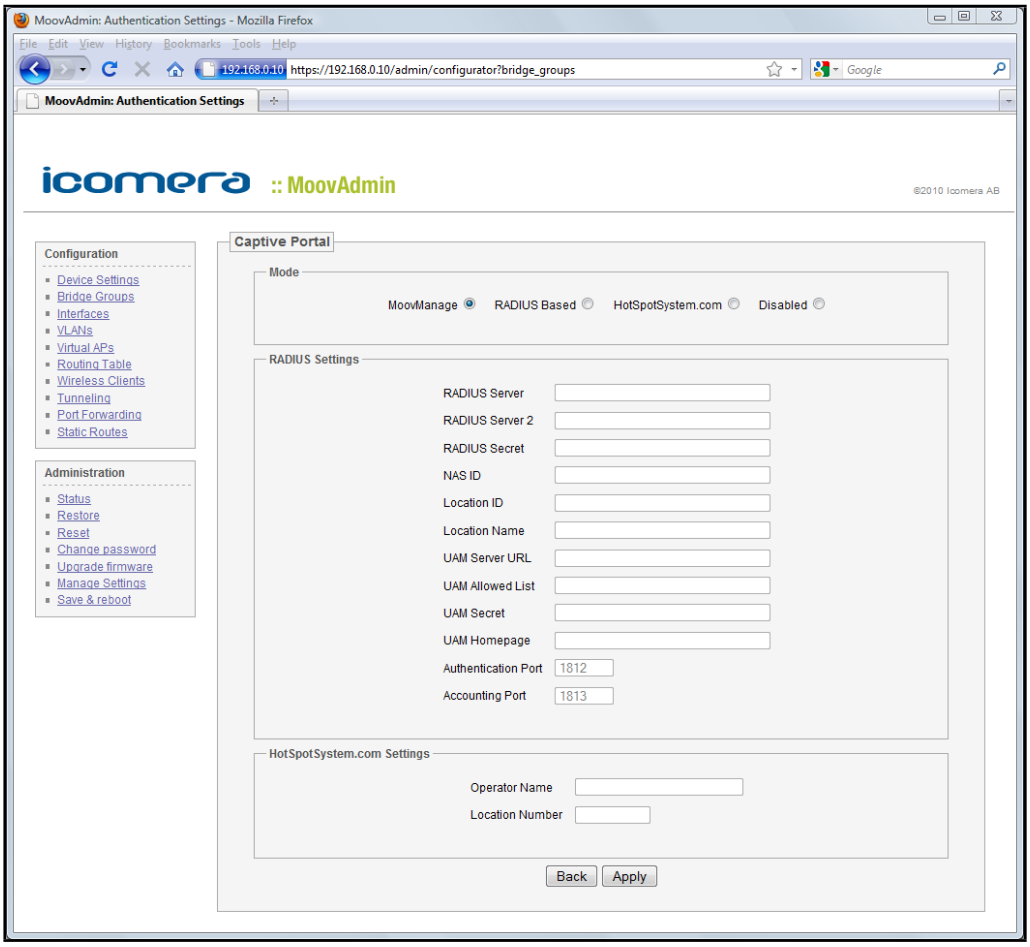
WAN Modem (M200 only)

This option is only available when the Dual WAN mode is set to bridge mode. You can use this option to select which WAN modem the internet traffic from this bridge group will pass though.

Proxy Server

The Moovbox supports forwarding http traffic through a web proxy server which can be enabled on a specified bridge group. To forward the traffic through a proxy server you must enable the proxy checkbox and enter the proxy server IP/Host address and port.

2.2 Captive Portal



This option enables you to set up a captive portal or splash page that users see when they try to access the network. This would typically be used in commercial Wi-Fi hotspot applications, and provides an opportunity to brand

the service and require users to agree to Terms and Conditions and/or an Acceptable Use Policy (AUP).

Note: A captive portal cannot be configured on the Default group; you will not see the Captive Portal option displayed. In order to implement a captive portal you must add at least one new bridge group, for example an access point.

Options are accessed from Bridge Groups -> Edit -> Edit Captive Portal.

The Moovbox supports three captive portal methods; MoovManage requiring no local configuration, a manual method with a user defined RADIUS and UAM servers and a managed service method hosted by a third party provider, HotSpotSystem.com. By default, the MoovManage Captive Portal option is enabled.

HotSpotSystem.com

Icomera has teamed with HotSpotSystem.com, a provider of a hosted hotspot service that enables you to quickly and simply set up your Moovbox to support voucher and credit/debit card billing. Support for their Instant Hotspot services is built into the Moovbox firmware; all you need to do is enter your Operator Name and Location Number in the fields provided. For more information about Instant Hotspot, please visit www.hotspotsystem.com.

Radius Based

Configuring a captive portal manually requires a RADIUS server for authentication and a web (UAM) server for hosting the portal pages. If you are a MoovManage subscriber, please use the MoovManage option.

The Moovbox can also be configured to work with third party captive portal solutions, and is compliant with WISPr, the Wi-Fi Aliance protocol for roaming between wireless Internet service providers. Please contact your Icomera Channel Partner or visit the Icomera support site for more information.

MoovManage

Icomera have simplified the Captive Portal feature on the Moovbox. If you have a MoovManage account a Captive Portal will have already been setup for you. To enable your MoovManage Captive Portal, simply select MoovManage, Apply the settings and save and reboot the device.

Note: If you wish to customize this portal; images and text, keeping the existing style, visit www.moovmanage.com, Configure $>$ Captive Portal. If you wish for a total portal redesign and/or questionnaire please send the pages written in html to moovbox.support@icomera.com for integration with our login scripts.

3 Interfaces

The Interfaces pane shows an overview of the physical Ethernet and Wireless interfaces of the Moovbox. To edit the physical interface settings click

the Edit button.

3.1 State

Set the state of the Moovbox's physical interfaces. "Off" (Wi-Fi only) disables the interface, "On" enables the interface. The Wi-Fi interface will act as an access point in this mode. The "WAN" option enables the interface as a WAN interface. The Wi-Fi interface will operate in client mode when used as a WAN interface.

3.2 Bridge Group

Set the physical interface to the required bridge group. This will set the physical interface in the specified group.

Tip: If you have configured a bridge group for Wi-Fi access with a captive portal enabled, the Wi-Fi interface must be assigned to this group. Icomera recommends that the Ethernet interface is always left on the default group as this is will still be available locally when the Moovbox is offline.

3.3 Wireless

The following options are only available when editing the Wi-Fi interface.

Mode

This option selects the 802.11 protocol required, e.g. choose '802.11b/g' for public Wi-Fi applications. This option will affect the radio channels and transmit powers available.

ESSID

In Wi-Fi wireless LAN computer networking, an extended service set identifier (ESSID) is a code attached to all packets on a wireless network to identify each packet as part of that network. The code is a case sensitive text string which consists of a maximum of 32 alphanumeric characters.

Tip: When configuring an Access Point set the ESSID to something meaningful, as this is the network name to which the clients will connect.

Hide ESSID

This option allows you to hide the ESSID from Wi-Fi users, and is useful when configuring a private Wi-Fi network which you do not want seen by casual Wi-Fi users.

Note: Don't hide the ESSID of a public Wi-Fi network otherwise users will not be able to connect.

L2 Isolation

The option prevents multiple Wi-Fi clients from communicating with each other when connected to the wireless access point.

Tip: Enabling this will prevent windows file sharing between clients. For better security, always enable this option on access points in public Wi-Fi networks.

Channel

This option enables you to choose the frequency in which the radio will operate. The channels that are available will vary depending on the 802.11 protocol specified in the mode section. When in WAN mode the channel can be set to "Any" which will cause it to scan all of the channels for an access point.

TX Power

This option enables you to set the transmit power of the Wi-Fi radio. The power must be set to conform to local regulations; check with your local telecommunications regulator if you are uncertain about Wi-Fi power restrictions in your region.

Encryption Type/Key & 802.1x

When using WEP or WPA with a pre shared key (PSK) you will need to enter an encryption key. When using WPA with the extensible authentication protocol (EAP) you may configure the 802.1x options in the 802.1x pane below.

3.4 WAN

These options are only available when the interface is used as a WAN interface. You can configure the the interface with a static IP, using DHCP or PPPoEs (Ethernet only).

IP Type

Select how the IP address will be allocated to the WAN interface. The options are a Static IP, DHCP or PPPoE (Ethernet only).

IP address

Set the IP address for the WAN interface (static IP only).

Subnet Mask

Set the subnet mask for the WAN interface (static IP only).

Default Gateway

Set the default gateway for the WAN interface (static IP only).

Primary DNS

Set the Primary DNS IP address for the WAN interface (static IP only).

Primary DNS

Set the Secondary DNS IP address for the WAN interface (static IP only).

Username

Set the username for a PPPoE connection.

Password

Set the password for a PPPoE connection.

LCP echo interval (seconds)

Set the LCP echo interval for a PPPoE connection.

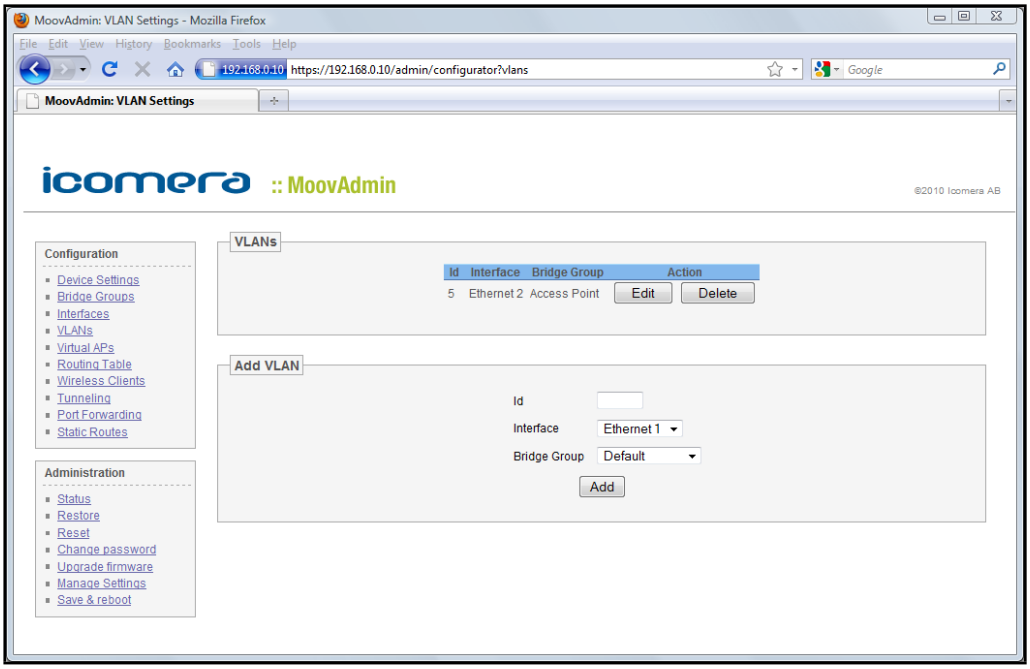
LCP echo number of failures

Set the LCP echo number of failures before reconnecting the PPPoE connection.

3.5 Isolating Third Party Devices for Security Purposes

In some circumstances, it is undesirable to allow Wi-Fi users to access the Ethernet interface of the Moovbox. For example, where a Moovbox is deployed on public transport to deliver Wi-Fi Internet access to passengers while also providing remote access to CCTV/DVR system. In this instance the Ethernet interface must be completely isolated to prevent a Wi-Fi user accessing the CCTV equipment. The Ethernet interface can be securely isolated from the Wi-Fi interface by assigning them to different bridge groups, and then setting up a VPN tunnel on the Ethernet interface bridge group. For more information about how to do this, please refer to the VPN Tunneling Reference Guide, available from your Icomera Channel Partner or as a download via Icomera's support site.

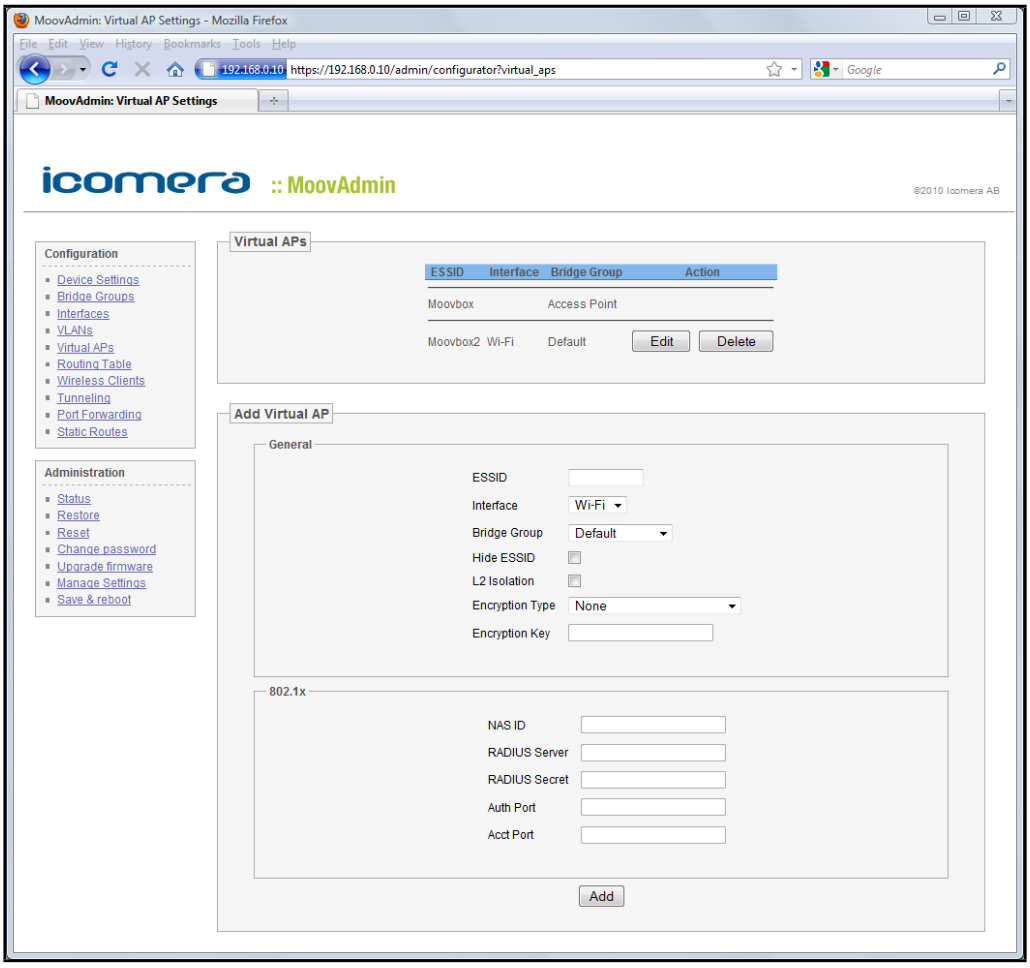
4 VLANs



The Moovbox will receive tagged packets and un-tag them for use within the network. The Moovbox will also tag any packets sent out in the specified bridge group.

Note: VLANs can only be applied to the Ethernet interfaces, and are used to segment traffic in a similar fashion to how Virtual APs are used on the Wireless interface. In vehicular applications, VLANs can be used for separating traffic from an IP-CCTV system and an on-board telematics system, for example.

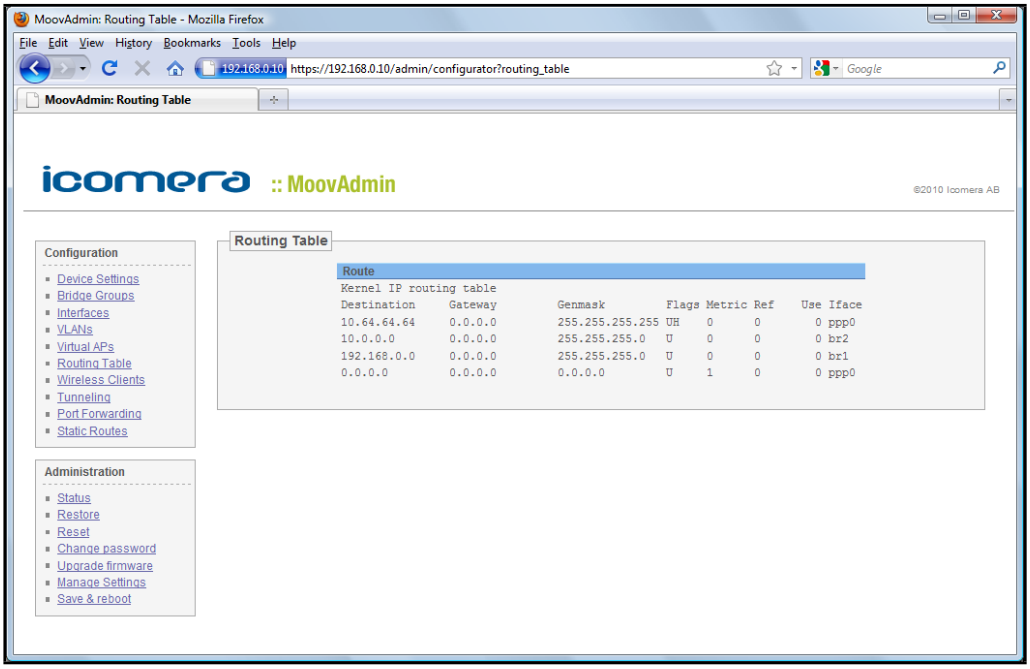
5 Virtual APs



The Moovbox supports multiple SSIDs on the wireless interface. This enables you to have more than one visible SSID from one Moovbox. Each SSID can be configured with a different bridge group giving a different client experience depending on which SSID to which they connect.

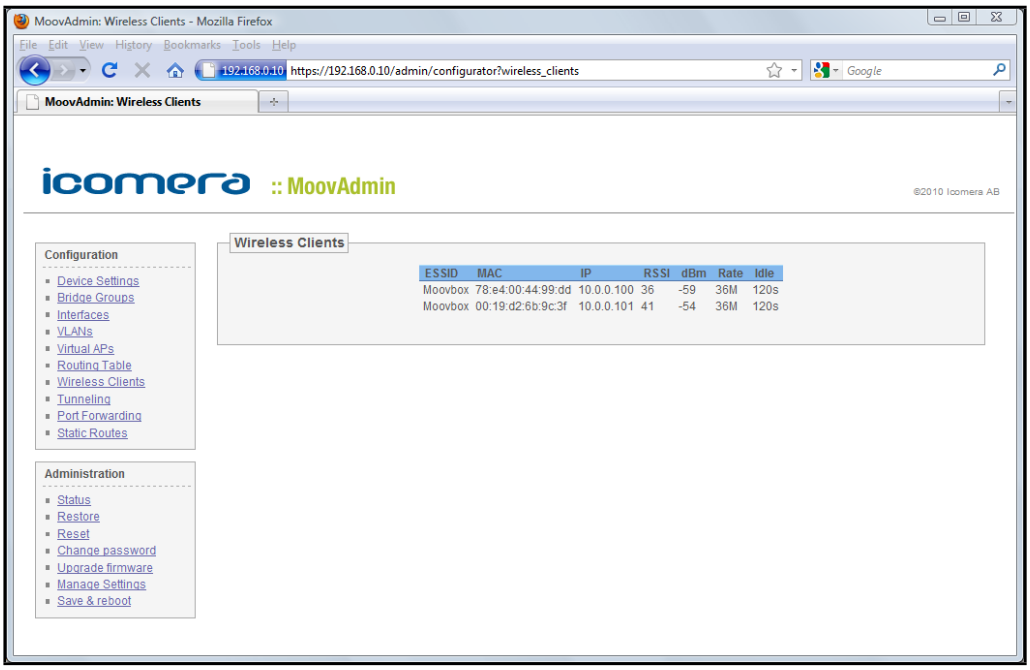
Note: Virtual APs can be used for deploying multiple commercial providers on the same access network. Similarly, virtual APs can be set up to accommodate devices such as wireless VoIP handsets that cannot negotiate a network connection using a captive portal.

6 Routing Table



The routing table shows all IP routes enabled across the Moovbox. This feature maybe useful when diagnosing IP issues for VPN and VLAN connectivity.

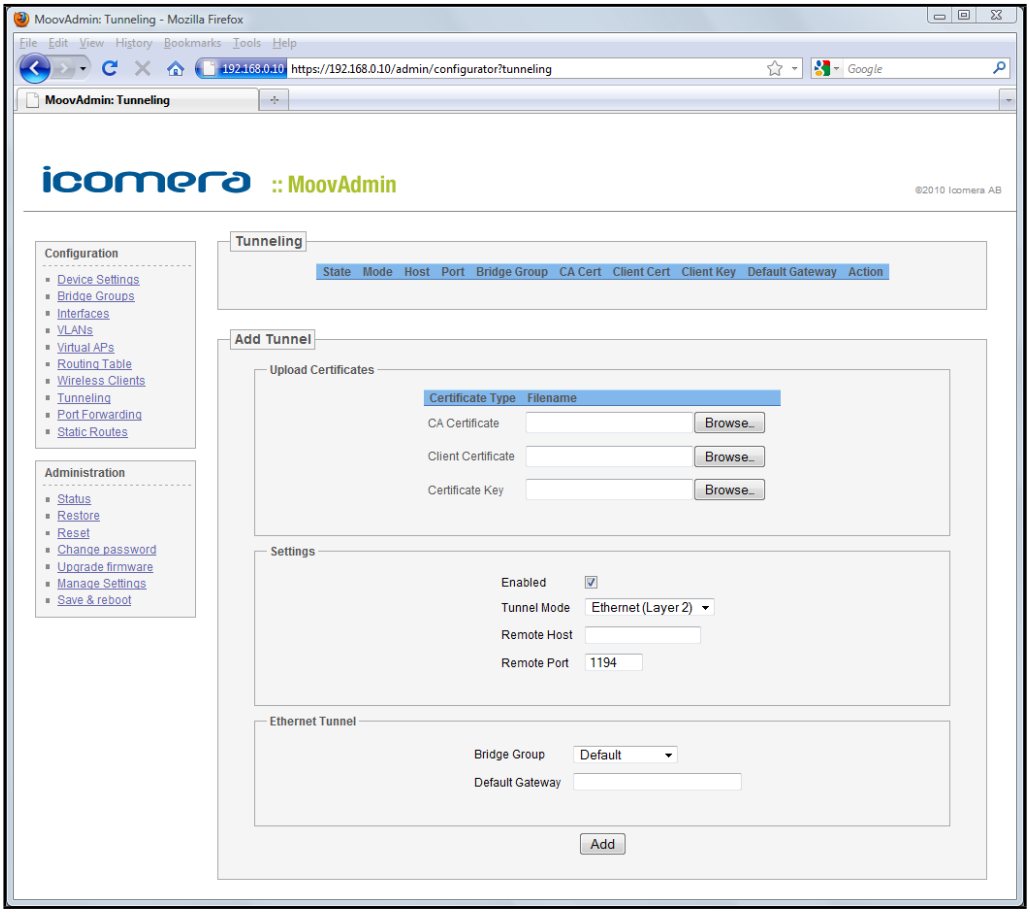
7 Wireless Clients



When a Wi-Fi client joins a Moovbox Wi-Fi network, it is displayed on the Wireless Clients screen. The table shows the SSID to which the client is associated the client device MAC address, and the IP address the device has been assigned via DHCP. The quality of the Wi-Fi connection is shown in three ways; the RSSI (Receive Signal Strength Indication), signal strength in dBm (decibels) and the Modulation Rate in Mbps at which the device is connected. In general terms the higher the number in dBm, the better the quality of the signal.

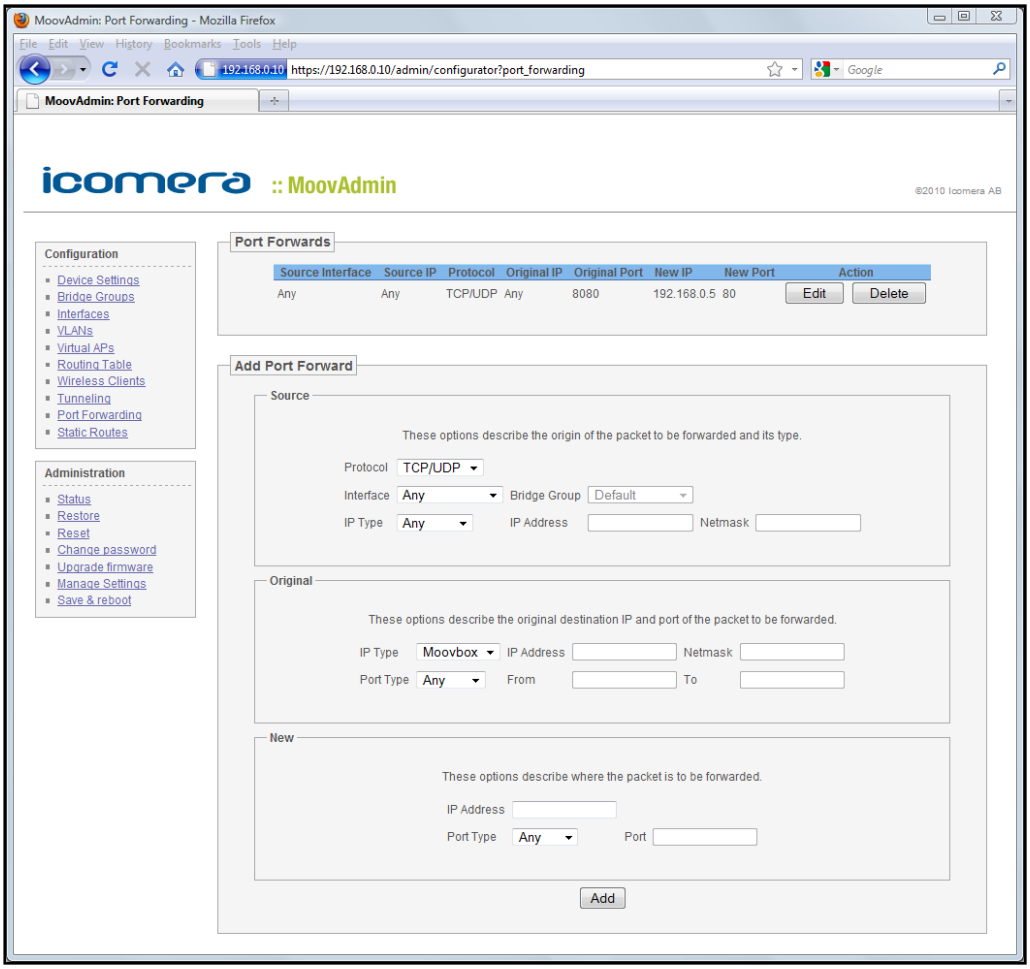
Note: You can use the Wireless Clients display to check Wi-Fi coverage when installing the Moovbox. Ensure that you can get good Wi-Fi signal reception; try using a higher gain or directional Wi-Fi antenna if the signal cannot reach certain areas.

8 Tunneling



The Moovbox supports multiple secure VPN tunneling so that it (and third party devices connected to it) can be accessed and controlled remotely in situations where a WAN static IP address is not available. For more information about how to configure the Moovbox for in-bound VPN tunneling, please refer to the VPN Tunneling Reference Guide, available from your Icomera Channel Partner or as a download via Icomera's support site.

9 Port Forwards



The port forwarding feature enables you alter the destination of any packet passing through the Moovbox based on a simple set of rules.

Common uses of this would be to forward a packet destined to the external interface of the Moovbox to the web interface of a device on the LAN or to forward any packet destined to port 25 to your own SMTP server.

9.1 Port Forwards

This section shows a list of port forwards currently configured on the system and the port forwards details. Next to each port forward are buttons which enable you to edit or delete the port forward.

9.2 Add Port Forward

Lets you add a new port forward to the Moovbox. The Source and Original sections are filters which select which packets are forwarded and the New section denotes where the packets should be forwarded to.

9.3 Source

These options describe a filter which matches the origin of the packet to be forwarded and its type.

Protocol

You should select the protocol of the packets to be forwarded.

Interface

Select the type of interface which the packets arrive at the Moovbox on.

Bridge Group

Select the bridge group which the packets arrive at the Moovbox on.

IP Type

Specify where the IP where the packets come from. Either any IP address (Any), a range of IP addresses (Network), or a single IP address (Host).

IP Address

If you set the IP type to host this is the source IP address. If you set the IP type to Network then this is the network address of the source subnet.

Netmask

Enter the subnet mask of the source subnet.

9.4 Original

These options describe a filter which matches the original destination of the packet to be forwarded.

This does not describe where the packets should be forwarded to. That is in the New section.

IP Type

Specify the IP where the packets to be filtered were originally destined. Either any IP address (Any), the Moovbox (Moovbox), a range of IP addresses (Network), or a single IP address (Host).

IP Address

If you set the IP type to host then this is the original destination IP address. If you set the IP type to Network then this is the network address of the original destination subnet.

Netmask

Enter the subnet mask of the original destination subnet.

Port type

Select the type of port to which the packet is originally destined. Either any port (Any), a single port (Single), or a range of ports (Range).

From

If you set the port type to Single then enter the port is here. If you set the port type to Range then enter the lower end of the range of ports.

To

Enter the upper end of the port range.

9.5 New

These options describe where the packets are to be forwarded to.

IP Address

Enter the IP address which the packets will be forwarded to.

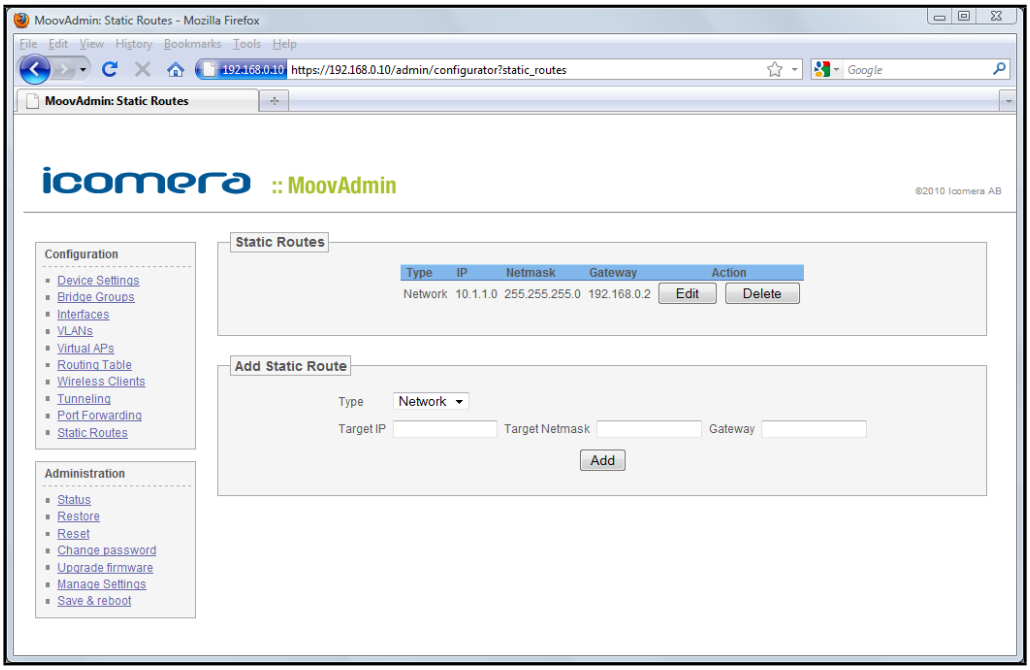
Port type

Select which port the packet is to be forwarded to. Either the same port it arrived on (Any), or a single port (Single).

Port

Enter the port the packet is forwarded to.

10 Static Routes



The static routes feature enables you to manually add static routes for networks and hosts.

10.1 Static Routes

This section lists the current static routes you have configured and allows you to edit and delete your existing static routes.

Static routes should be considered an advanced feature and only used if you are very familiar with IP routing.

10.2 Add Static Route

Lets you add a new static route to the Moovbox.

Type

Select “Network” if you wish to route traffic to a network block or “Host” if you are only routing traffic to a single host.

Target IP

Enter the network IP address of the network or the IP address of the host you are routing.

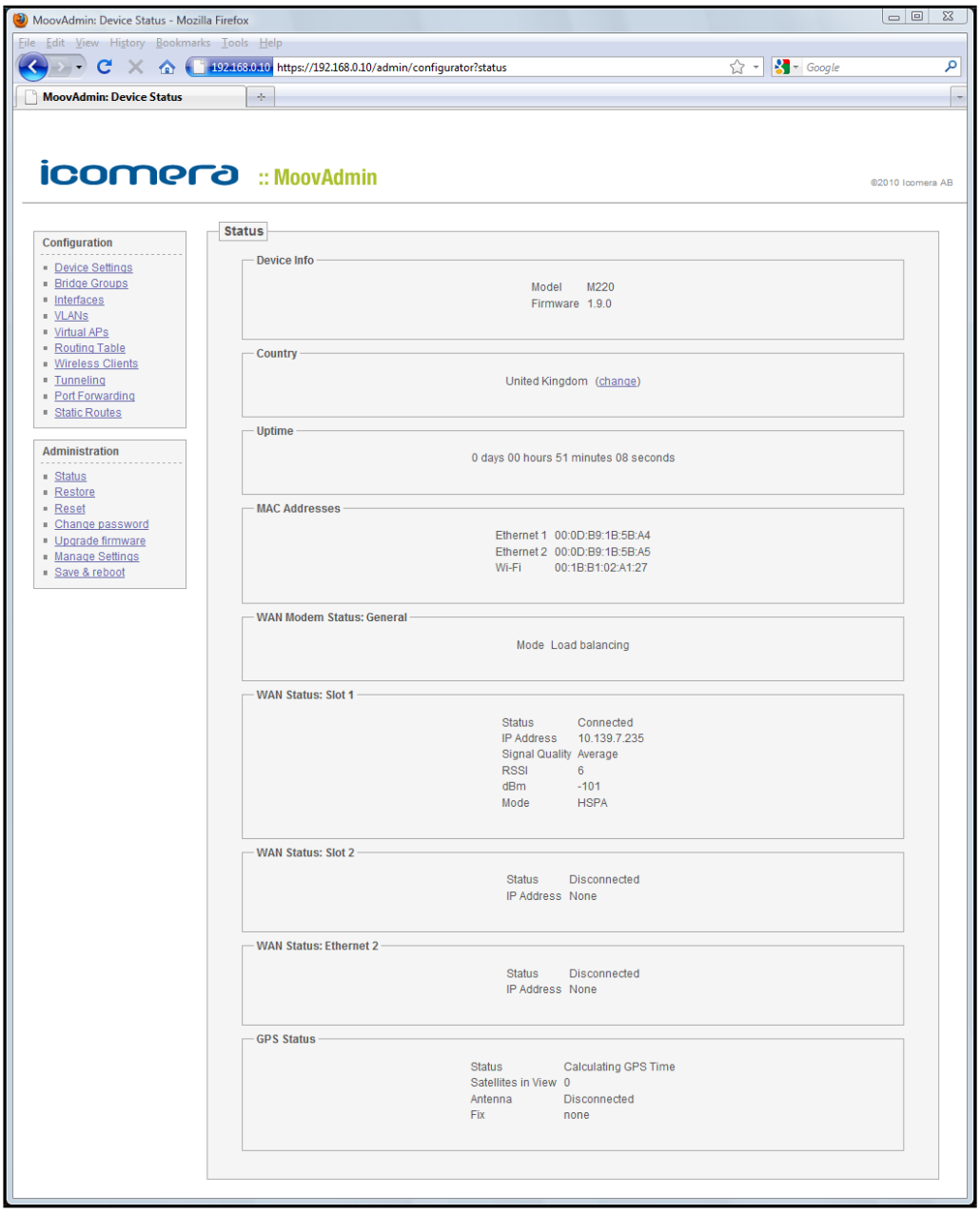
Target Netmask

Enter the subnet of the network you are routing.

Gateway

Enter the IP address of the netowrk gateway which the traffic is to be routed through.

11 Status



The Status window shows the firmware version loaded on the Moovbox, the time passed since the device was booted, and the MAC addresses of the

LAN and WLAN interfaces. The WAN Modem Status pane provides information about the quality of the WAN link. This can be helpful when using the Moovbox to survey your service provider's coverage. The GPS Status pane shows whether or not your Moovbox has obtained a GPS fix, and the location accurate to within 5–8 meters horizontally and 10–16 meters vertically.

12 Restore

Restore reset all the settings changed in the current session to the current running configuration.

Tip: Before you make any changes to the configuration of the Moovbox, always restore the running configuration to avoid any unexpected changes to be committed.

13 Reset

Reset clears the configuration completely and resets the Moovbox back to the factory default.

Tip: The IP address on the Ethernet interface, the username and the password will be reset back to factory default; IP address: 192.168.0.10/24, username: admin, password: password

14 Change Password

Enter the new password twice; note the password is case sensitive. Icomera recommends all passwords are changed from factory default.

Tip: Do not lose this password. If you lose the password and are unable to log on to the Moovbox and are using firmware 1.4.8 or later, you may use the Moovbox Recovery Tool to recover your device. This software is available for download from the Icomera support site. If you are using older firmware, you will need to return the product for factory resetting. Contact your supplier for more information.

15 Upgrade Firmware

Upgrade the firmware by choosing a file to upload to the Moovbox; this should take about three minutes if the firmware image is uploaded from your local machine over the Ethernet connection.

Tip: Always make sure you are upgrading the Moovbox with a valid version of firmware. If upgrading remotely (for example over the public Internet on broadband) the upgrade speed will vary depending on your speed of your uplink to the Moovbox.

16 Manage Settings

Manage Settings gives you the ability to download and upload configuration files. The Moovbox has two configurations: ‘running configuration’ (configuration on boot up), and ‘current configuration’ (the configuration with the changes made in MoovAdmin). The current configuration is not written to the running configuration until the Moovbox is saved and rebooted.

☞ ***Tip:*** When downloading a settings file, you are downloading the current configuration of the Moovbox not the running configuration. If you wish to download the running configuration, restore the settings before downloading. Icomera recommends before any configuration changes are made, the configuration is backed up.

17 Save & Reboot

If changes have been made the Moovbox must be saved and rebooted before the changes will take effect. If changes have been made to the Moovbox and it is only rebooted, all the changes will be lost.

☞ ***Tip:*** If you make any changes which lock you out of the Moovbox you may use the Moovbox Recovery Tool to recover your device. This software is available for download from the Icomera support site.